What is claimed is:

1. A computer-readable medium having computer-executable instructions for operating a policy agent of a network for performing steps comprising:

detecting a network connection from a client computer on the network;

composing a challenge for authenticating a user of the client computer associated with said network connection, the challenge being encrypted with a private key of the policy agent;

transmitting the challenge to the client computer;

receiving a response from the client computer;

decrypting the response using a public key of the user to obtain a first message digest value;

receiving network data through the network connection with the client computer;

calculating a second message digest value based on the challenge and the received network data;

comparing the first and second message digest values to determine whether a match is found.

2. A computer-readable medium as in claim 1, wherein the policy agent is a firewall.

3. A computer-readable medium as in claim 1, wherein the step of composing including encrypting the challenge with a public key of the user.

4. A computer-readable medium as in claim 3, wherein the step of decrypting includes decrypting the response with a private key of the policy agent.

5. A computer-readable medium as in claim 1, wherein the step of composing includes generating a third digest value from data including a time value, and encrypting the third digest value with the private key of the policy agent.

6. A computer-readable medium as in claim 1, wherein the received network data are in a form of packets, and the step of calculating calculates the second message digest value based on a pre-selected number of packets of the received network data.

7. A computer-readable medium as in claim 1, having further computer-executable instructions for performing network access policies on the received network data according to the identity of the user after a match between the first and second message digest values is found.

8. A method of authenticating a user using a client computer on a network to transmit network data through a policy agent of the network, comprising the steps of:

detecting by the policy agent a network connection from the client computer for transmitting network data of the user;

receiving by the policy agent network data transmitted through the network connection from the client computer;

obtaining, by the policy agent, identity of the user and a public key of the user;

composing, by the policy agent, a challenge encrypted with a private key of the policy agent;

sending the challenge to the client computer;

decrypting, by the client computer, the challenge;

generating, by the client computer, a first message digest value based on the challenge and the network data of the user;

encrypting, by the client computer, the first message digest value with a private key of the user to create a response;

sending the response to the policy agent;

decrypting, by the policy agent, the response to obtain the first message digest value;

calculating, by the policy agent, a second message digest value based on the challenge and the network data received through the network connection from the client computer;

comparing the first and second message digest values to determine whether there is a match therebetween.

9. A method as in claim 8, further including the step of applying network policies by the policy agent on the received network data based on the identity of the user after a match between the first and second message digest values is found.

10. A method as in claim 8, wherein the step of composing the challenge includes encrypting the challenge with the public key of the user.

11. A method as in claim 8, wherein the step of encrypting by the client computer includes encrypting the first message digest value with a public key of the policy agent.

12. A method as in claim 8, wherein the step of composing the challenge includes generating a third message digest value based on data including a time value and encrypting the third message digest value to from the challenge.

13. A method as in claim 8, wherein the received network data are in a form of packets, and the step of generating by the client computer generates the first message digest value based on data of a pre-selected number of packets of the received network data.

14. A method as in claim 8, wherein the step of generating by the client computer generates the first message digest value based on a random number, data decrypted from the challenge, and data of the pre-selected packets of the received network data.

15. A method as in claim 8, wherein the policy agent is a firewall of the network.